D7.4 Recommendations on Standards Evolution

Project number:	644080
Project acronym:	SAFURE
Project title:	SAFURE: SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems
Start date of the project:	1st February, 2015
Duration:	36 months
Programme:	H2020-ICT-2014-1

Deliverable type:	Report
Deliverable reference number:	ICT-644080 / D7.4 /1.0
Work package	WP 7
Due date:	May 2018 – M40
Actual submission date:	30th May, 2018

Responsible organisation:	ESCR
Editor:	André Osterhues
Dissemination level:	PU
Revision:	1.0

Abstract:	This document gives recommendations on the evolution of existing standards.
Keywords:	Security, safety, standards, telecommunication, automotive

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080.

This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

Editor

André Osterhues, main editor (ESCR)

Contributors/Reviewer (ordered according to beneficiary numbers)

André Osterhues (ESCR)
Stefania Botta (MAG)
Edin Arnautovic (TTT)
Don Kuzhiyelil (SYSG)
Jonas Diemer (SYM)
Sylvain Girbal (TRT)
Robin Hofmann (TUBS)
Marco Di Natale (SSSA)
Rehan Ahmed (ETHZ)
Dominique Ragot (TCS)

Disclaimer

Executive Summary

This document provides information on applicable standards in the context of mixed-critical cyber-physical systems and gives recommendations on the evolution of these standards.

We have compiled the most relevant existing standards and incorporated recommendations that could be considered in future versions of these standards. Besides generic standards, also domain-specific standards for the telecommunications and automotive domains are addressed.

Contents

Chapter 1 Recommendations

In this chapter, standards relevant for the SAFURE project are summarized.

For some standards, a new version was published during the run-time of the project, reflecting the advances in technology. These are shortly summarized here.

Furthermore, during the project, we noticed that some standards could be improved with respect to our research results. Therefore, we collected recommendations for future versions of these standards, which are presented here.

This chapter is split according to different industry domains. We start with generic standards in section 1.1, then continue with modelling in section 1.2, and finally come to telecommunications (1.3) and automotive (1.4) standards.

1.1 Generic

1.1.1 Safety

In addition to very specific safety standards in the military domain, civilian standards also exist, with first the IEC 61508 [4] generic industry standard, as well as sector-specific standards such as the CENELEC Standard EN 50126 [5] for railways, the ISO 26262 [3] standard for automotive, and the DO-178 [1] and the DO-254 [2] standards in avionics.

These standards have already been presented in Section 5.3 of Deliverable D7.3. Consequently, in this section, we will primarily focus on practices specific to mixed-critical cyber-physical systems that SAFURE particularly targets. As SAFURE has two dedicated automotive use-cases, the recommendations with regards to ISO 26262 are presented in a dedicated section.

IEC 61508

Based on the analysis of Nordhoff [7], within ISO 61508 [4] Part 3 there are already some parts that fit together well with compositional embedded security such as MILS, for example the specification of ""any safety-related or relevant constraints between the hardware and the software" (7.2.2.7), to "clearly identify the non-safety functions" (7.2.2.9), identification of "functions related to the detection, annunciation and management of faults in the software itself (software self-monitoring)" (7.2.2.10, by use of MILS health monitoring provided by the MILS operating system), to fulfil "independence requirements between functions" (7.2.2.10), and to analyse "best case and worst case execution time" (7.2.2.12, the analysis is simplified by using time partitioning).

Part 3, section 7.4.3.2.b of this standard, states that a software architecture shall "be based on a partitioning into elements/subsystems", moreover a focus of software architecture (7.4.3.2.c) is to "determine all software/hardware interactions and evaluate and detail their significance". The use of a MILS operating system by design gives a technical separation into partitions and all software/hardware interactions can be traced to the level of partitions.

Part 3, Section 7.4.2, is dealing with software design requirements, here MILS is particularly useful for "abstraction, modularity and other features which control complexity", "the expression of ... information flow between elements, ... timing constraints" (7.4.2.2). MILS is a feature that "facilitates software modification" (7.4.2.4), and it allows to "keep the safety-

related part of the software simple" (7.4.2.6, by factoring out the safety-related part of software into a high-criticality partition), and provides "adequate design measures ensure that the failures of non-safety functions cannot adversely affect safety functions" (7.4.2.8), "unless adequate independence between the safety functions of the different safety integrity levels can be shown in the design" (7.4.2.9, use a MILS platform to justify independence).

However, architectural information is quite dispersed in IEC 61508 and IEC 61508 could absorb from the ISO / IEC 15408 (Common Criteria [8]) the way that a methodological analysis of architecture (domain separation, initialisation, self-protection and non-bypassability) is sketched in Common Criteria [8], Part 3, Section 13.1 (pages 97-98). A practical way to work out such as "architectural perspective" for IEC 61508 could start with mapping the partitioning described as "independence of execution" and also "non-interference" in IEC 61508 Part 3, Annex F to the IEC 61508 Part 3, Section 7 elements we have mentioned, either in form of a checklist or in the form of free-from guidance. The goal would be to describe, in that Annex F, how an architecture-based evaluation approach could be used to describe IEC 61508 conformance. Thinking this further, amending IEC 61508 by a MILS / composite system annex, for instance could create a niche market for "Annex-F"-based IEC 61508 system evaluations.

DO-297 & DO-254

Avionic safety standards are defining different Design Assurance Levels (DAL), determined from a safety assessment process[1] and a hazard analysis[2]. A classification is performed by assessing the effects of a failure condition on the aircraft, its crew or the passengers.

Ensuring correctness and guaranteeing deadlines is critical to certify airborne systems. To do so, the standards emphasize the practice of both spatial and time partitioning. Such partitioning techniques do not cope well with mixed-critical systems that aim at co-running different applications with different safety levels. These standards were defined prior to the multi-core era that has a significant impact on time partitioning, and this do not properly address multi-criticality.

Avionic standards updates: Multi-cores are currently a challenge for the avionic industry with regards to their impact on time partitioning. In SAFURE, we see mixed-critical systems as an opportunity to overcome this challenge. Within SAFURE, we developed the BB-RTE Run Time Engine that aims at guaranteeing high-critical task timing behaviour (aka deadlines) while suspending low critical tasks when they are endangering real-time behaviours of high-critical tasks.

For such a process to be in accordance with the standards, a few constraints need to be relaxed: Currently, the standards require strict partitioning between the application of different safety levels. We need to relax this constraint to allow high-critical tasks to possibly impact low-critical tasks, as the latter could be suspended to guarantee the former time behaviour.

On the other hand, the timing impact of low-critical tasks on the high-critical ones is effectively bounded by the run-time engine that will have to be certified.

[1] ARP4761, see https://en.wikipedia.org/wiki/ARP4761

[2] https://en.wikipedia.org/wiki/Hazard_analysis

1.1.2 Security

ISO/IEC 15408 (Common Criteria)

The Common Criteria for Information Technology Security Evaluation (Common Criteria) define a framework for the specification and certification of a computer security system.

Currently, there is no Protection Profile for Automotive Ethernet Network. Within the SAFURE project, we have created an experimental Protection Profile for Automotive Ethernet Network (see deliverable D5.3).

MILS Separation Kernel Standardization Effort

In addition to the Open Group, the EURO-MILS «MILS Architecture Template» and the MILS community (now housed at http://mils.community/) already mentioned in SAFURE D7.3, a new relevant standardisation effort has started at the CCUF (Common Criteria Users' Forum, http://www.ccusersforum.org/). At the April 2018 CCUF meeting at Trondheim there was a break-out for separation kernels about forming a CCUF working group for separation kernels. The working group would follow the guidelines for international technical communities and collaborative protection profiles [9]. That is, the CCUF working group starts to produce an «Essential Security Requirements» (ESR) document that, as a basis for further discussions, explains how to describe common properties of a separation kernel in plain (i.e. non CC-specific) language that is understandable to a wider audience. For example, at that April 2018 meeting, initial discussions were about ESR naming conventions, and it was suggested to take CPU pinning into account. If things work out well, the ESR will be the basis for further CC standardisation of a collaborative protection profile for separation kernel. From the SAFURE consortium, so far partner SYSG is following the CCUF separation kernel process, which is open to any interested party.

Hence, for MILS systems there is currently an ongoing standardization opportunity at CCUF, and SYSGO will bring in its lessons learnt while building the demonstrators in SAFURE. For example, SAFURE contributes with pragmatic solutions to some concrete problems such as Secure Boot.

As far as the Common Criteria as a whole are concerned, it is harder to give a generic recommendation. In the context with the secure boot SAFURE research topic, it could be worth noting that the approach of modular protection profiles that had been introduced with the current Version 3.1, revision 5, of the CC, is probably also quite useful for separation kernels: for example, not every separation kernel has secure boot for every target that it might be running on, so it might be wise to keep this component modular. Perhaps future CC versions also could benefit from providing more guidance on the evaluation (ADV/ATE/AVA) of separation-kernel-based composite architectures, even where a formal CC composition approach is not being followed.

1.1.3 Temperature and Energy

Currently, temperature sensors are a non-privileged resource in Android OS. Research in SAFURE project has shown that this poses a security risk in the form of thermal covert and side channels. Therefore, temperature sensors should be subject to access restrictions.

Power sensors should also be access restricted due to the feasibility of power covert channels.

1.2 Modelling

SysML and UML (MARTE)

The Object Management Group or OMG, the organization that is responsible for the definition of standards for Object-Oriented modeling has recognized since the 90s that the embedded domain requires models for the definition of time, scheduling and performance-related constraints and attributes.

The original profile SPT (Schedulability Performance and Time) evolved (starting from 2004) in the MARTE profile, where MARTE stands for Modeling and Analysis of Real-Time Embedded systems.

The MARTE profile is quite large (more than 700 pages), but does not cover the full spectrum of issues related to the timing analysis for mixed-critical systems and ignores issues related to security and classical safety.

MARTE is formally based on UML. However, almost at the same time a new language derived from UML, namely SysML, was proposed for the definition of system-level models (UML is restricted to the model of software subsystems and components).

Most of MARTE is applicable with minor changes to SysML as well.

In SAFURE, and more precisely in WP2, as documented in D2.2, we propose a set of metamodels, profiles and stereotypes that are applicable to embedded systems and could be considered for a future extension to MARTE to consider mixed-critical systems.

Also, of particular interest is the discussion of metamodels and extensions for security, and the joint consideration of both aspects (safety and security) in the same context.

All the metamodels and modeling extensions proposed in SAFURE have been presented and made available on standard tools and making use of standard languages (MOF on Eclipse) so that they can be easily analyzed, adopted or modified.

In addition, we provided profiles for UML and SysML for IBM Rhapsody, which is probably the most common tool on the market.

While the members of SAFURE are not currently part of the OMG and the standardization group that is in charge of MARTE, we do have continuous exchange of information with the leaders of such groups and initiatives from conferences, workshops and technical meetings.

AUTOSAR

AUTOSAR is a standard maintained by an industry alliance with the same name and restricted to automotive manufacturers and suppliers. AUTOSAR is a standard for component-based development for automotive software that includes the definition of a modeling language, a standardized architecture with all its basic SW components (Operating System, drivers, communication), and a standard API for communication and interoperability (Run-Time Environment).

In the context of SAFURE, the some limitations of the AUTOSAR modeling framework towards security, time and safety have been discussed in WP2, and in D2.2, we identified several possible solutions for deadline with these limitations with extensions to the modeling language.

The extensions have been prototyped in Rhapsody and Artop (two tools with AUTOSAR modeling capabilities) and were also analyzed with respect to the potential for better analysis and synthesis.

1.3 Telecommunications Domain

IEEE 802.1Q

The IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks describes how the Media Access Control (MAC) Service is supported by Bridged Networks, the principles of operation of those networks, and the operation of MAC Bridges and VLAN Bridges, including management, protocols, and algorithms.

With the introduction of the Time-Sensitive Networking (TSN) group, new mechanisms have been introduced to IEEE802.1Q, which are intended to provide increased reliability and deterministic quality of services for real-time Ethernet traffic. Several of the TSN standards have already been evaluated in the context of SAFURE, while others are still in development. The ongoing evaluation has shown, that the standards by themselves cannot provide any timing guarantees and formal analyses are required to evaluate the worst-case behaviour of a standard.

5G

Although 5G is not expected to be massively deployed before 3 to 5 years, it is interesting to show the large number of new services available, provided that the terminals (mobile phones, tablets, etc.) are not locking-up these services for already existing large players, but enable third parties to deploy these services independently from the actual platform providers. There, standardization, regulation, and certification have a role to play to maintain fair competition in these new markets.

The ARCEP report [6] gives an overview of upcoming 5G features such as:

- Use-case (figure 5 on page 10)
- Technologies such as IoT waveforms (page 17)
- Mobile CDN, MEC and device-to-device (page 19)

1.4 Automotive Domain

AUTOSAR

AUTOSAR (AUTomotive Open System ARchitecture) is a worldwide development partnership of vehicle manufacturers, suppliers and other companies from the electronics, semiconductor and software industry.

AUTOSAR Adaptive

The Adaptive Platform is AUTOSAR's solution for high-performance computing ECUs to build fail-operational systems.

AUTOSAR Adaptive Platform will provide a bridge to solution for a new class of future automotive applications and products (especially targeting remote updates, third-party applications, autonomous driving, etc.). AUTOSAR Adaptive Platform will determine a way in which automotive SW will be developed in the near future to be integrated in the automotive SW ecosystem.

With this goal, the Adaptive Platform has to bridge the gap between high-performance requirements, flexibility and safe and secure systems. The results developed in SAFURE address many of these topics and should be proposed for inclusion.

AUTOSAR RTE Generation

A part of the AUTOSAR process that is also affected by the SAFURE project is the generation of the RTE.

The RTE is the software layer that is in charge of the communication between the system functions, and of the scheduling (after the creation of a task model). In classic AUTOSAR, the RTE is statically generated as the result of a synthesis process that considers the constraints acting on the system functions.

The synthesis process of the RTE, however, currently does not consider two fundamental issues that are of primary interest for mixed-critical systems.

The first is the encryption of data on communications that are characterized by security requirements.

In D2.2, we addressed the definition of such security requirements in the context of an AUTOSAR model, and later we outlined the mechanisms that could lead to an RTE implementation with the automatic generation of code that performs encryption in the context of communication.

In D4.3, D6.5 and D6.6 we outlined a process by which AUTOSAR runnables and tasks may be annotated with a criticality attribute and we explained how this criticality definition could lead to the synthesis of an RTE task code that also includes calls to the AUTOSAR OS API for timing protection and isolation. In this way, the isolation can be guaranteed for systems subject to ISO26262 in an AUTOSAR flow.

ISO26262

The ISO26262 standard on automotive safety [3] requires freedom from interferences, which has been implemented at firmware level, covering both **timing protection** and **memory and exchange of information protection**.

Timing protection is typically implemented using static approaches like time-triggered scheduling, cyclic execution scheduling and fixed priority-based scheduling. In SAFURE, we have also analysed dynamic scheduling approaches.

With respect to **memory and exchange of information**, ISO 26262 mandates the protection against corruption of data as well as against read/write access from another software element. This is typically implemented using memory protection, parity bits, error-correcting codes (ECCs), and cyclic redundancy checks (CRCs). To offer even stronger protection than CRCs, we suggest using cryptographic data integrity protection mechanisms such as MACs or digital signatures, which additionally cover security requirements, thus achieving synergy effects between safety and security.

See deliverables D4.2, D4.3 and D6.2 for details.

SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems)

This best-practices guidebook gives a foundation for the development of next standard regarding vehicular security based on identified practices in the industry. SAFURE project has also identified and demonstrated several practices including encryption and authentication on the application level to ensure end-to-end security of exchanged messages.

ISO/SAE 21434 (Road Vehicles – Cybersecurity engineering)

This future standard should define security concepts for automotive industry and specify the requirements on the security process including the criteria for the assessment of this process. In addition, it should present the state of the art regarding automotive security.

SAFURE results cover current state of the art and can serve as a reference within this standard.

Chapter 2 Summary and Conclusion

In this document, we have compiled the standards that are relevant for mixed-critical cyber-physical systems. We have summarized existing standards and incorporated recommendations that could be considered in future versions of these standards. We have addressed several generic standards, but also domain-specific standards for the telecommunications and automotive domains.

List of Abbreviations

Abbreviation	Explanation
API	Application Programming Interface
AUTOSAR	Automotive Open System Architecture
CC	Common Criteria
CCUF	Common Criteria Users' Forum
CENELEC	European Committee for Electrotechnical Standardization
CRC	Cyclic Redundancy Check
DAL	Design Assurance Level
ECC	Error-Correcting Code
ECU	Electronic Control Unit
ESR	Essential Security Requirement
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
MAC	Media Access Control
MAC	Message Authentication Code
MARTE	Modeling and Analysis of Real-Time Embedded systems
MILS	Multiple Independent Levels of Security
OMG	Object Management Group
OS	Operating System
RTE	Run-Time Environment
SAE	Society of Automotive Engineers
TSN	Time-Sensitive Networking
UML	Unified Modelling Language

Bibliography

[1] DO-178B: Software Considerations in Airborne Systems and Equipment Certification. Radio Technical Commission for Aeronautics (RTCA) and EURopean Organisation for Civil Aviation Equipment (EUROCAE). 1992.

[2] DO-254: Hardware Considerations in Airborne Systems and Equipment Certification. Radio Technical Commission for Aeronautics (RTCA) and EURopean Organisation for Civil Aviation Equipment (EUROCAE). 1992.

[3] ISO 26262: Road Vehicles - Functional Safety. International Organization for Standardization (ISO). 2011.

[4] IEC 61508: Functional Safety of Electrical, Electronic, or Programmable Electronic Safety-related Systems. International Electrotechnical Commission. 2011.

[5] EN 50126: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). European Committee for Electrotechnical Standardization (CENELEC). 2012.

[6] 5G: Issues & Challenges. Autorité de Régulation des Communications Électroniques et des Postes (ARCEP). March 2017. http://www.arcep.fr/uploads/tx_gspublication/Report-5G-issues-challenges-march2017.pdf

[7] Nordhoff, Sven, Blasum, Holger, Ease Standard Compliance by Technical Means via MILS, MILS workshop 2017, https://doi.org/10.5281/zenodo.571175.

[8] Common Criteria Sponsoring Organizations, Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 5, vol. 1--3, April, 2017, http://www.commoncriteriaportal.org/cc/.

[9] “Establishing ITCs and CPP Development - v0-7.Pdf.” Accessed May 14, 2018. https://www.commoncriteriaportal.org/files/communities/Establishing%20iTCs%20and%20cPP%20development%20-%20v0-7.pdf.